DRAFT

COUNCIL OF TECHNOLOGY SERVICES (COTS)
SECURITY WORKGROUP
MINUTES
January 16, 2003
Department of Rehabilitative Services Conference Room
3:00 PM

ATTENDANCE:

Members:

Ernie Steidle, Department of Rehabilitative Services (DRS), Co-Chair; Peter Berinato, Department of Social Services (DSS); Merritt Cogswell, Department of Accounts, State Internal Auditor, (SIA/DOA); Taz Daughtery, James Madison University (JMU); Dan Galloway, James Madison University (JMU); Don Kendrick, Department of Information Technology (DIT); Paul Lubic, Department of Technology Planning (DTP); John Payne, DRS; Shirley Payne, University of Virginia (UVA); Chuck Tyger, Department of Technology Planning (DTP).

Guests and Staff:

Guests

Jenny Hunter, COTS Executive Director; and Mark Samblanet, Telos Corporation

Staff

Eric Perkins, Department of Technology Planning (DTP)

WELCOME AND OPEN REMARKS:

Co-Chair Ernie Steidle welcomed the members and guests, and advised that the following new members have joined the Workgroup: Peter Berinato, DSS; Joe Connor, Virginia Employment Commission (VEC); Dan Galloway, JMU; Kenny White, Virginia Department of Health (VDH).

APPROVAL OF MINUTES:

The December 10, 2002 Minutes were amended as follows: Taz Daughtery's affiliation was correct to "JMU," and Shirley Payne's status was change to "member." The minutes were adopted as amended.

WORKGROUP CHARTER:

Ernie Steidle discussed changes made to the Charter at the request of Joy Hughes (GMU) during the January 9, 2003 meeting of COTS. Following a general discussion it was agreed by the members to add George Mason University's Center for Secure Information Systems (CSIS) to the list of security experts mentioned in the Workgroup Mission, as well as to the second bullet in the Short-Term Objectives and Deliverables section. The revised draft of the Charter will be available during the month of February for review and comment on DTP's Online Review and Comment Application (ORCA) Web site. Following the review period, the draft Charter will be provided to COTS for approval at their March meeting.

VIRGINIA ALLIANCE FOR SECURE COMPUTING AND NETWORKING:

Shirley Payne's presentation introduced the Virginia Alliance for Secure Computing and Networking to the Workgroup. The Alliance is comprised of security practitioners from GMU, JMU, and Virginia Tech. Its purpose is to strengthen security programs across Virginia higher education by integrating and making available field-proven tools, best practices, and people from partnering institutions. The Alliances intends to expand its scope to offer similar services to state agencies and local governments. Their planned offerings include security training, consulting, Web-based toolkit, and expansion of the existing higher education VA-CIRT group for incident alerts and reporting.

Deleted: Charter¶
Department of Rehabilitative Services¶
¶
DRAFT MINUTES

Deleted: December 10, 2002

Deleted: Participants

Deleted: John Payne, Department of Rehabilitative Services (DRS); Merritt Cogswell, State Internal Auditor, (DOA); John Palese, Department of Social Services (DSS); Shirley Payne, University of Virginia (UVA); Jenny Hunter, ____;

Deleted: Eric Perkins, Department of Technology Planning (DTP); Taz ___, Daughtry, James Madison University (JMU); Harry Sutton, Department of Social Services (DSS) ;

Deleted: ; Ernie Steidle, Department of Rehabilitative Services (DRS), and Linda Taylor, Department of Rehabilitative Services (DRS)

Deleted: ¶

Deleted: General Information:¶
¶
Ernie

Deleted: ¶

Deleted: <#>Sites Documents available on the shared site are: Charter Development Draft, COTS Security Workgroup Presentation and several other drafts and products available for review. The site is designed for the Workgroup to communicate with one another. ¶
<#>Teleconferences will be offered to individuals who cannot attend the meetings. A video teleconferencing studio will be installed at DRS conference rooms probably in the Spring. ¶
<#>Today's meeting is to help one decide whether you would like to be a member of the Security Workgroup. Ernie will submit the names of the individuals who are interested in being a member to the COTS executive committee and obtain the ruling how to constitute a workgroup to become a permanent memberapproval. ¶
<#>Ernie will reviewmember's homework in the shared document to be completed. ¶

Deleted: HISTORY

Deleted: COTS have has existed for a long time—there are eight or nine workgroups. One of the workgroups that produced products relative to technology security is the COTS Enterprise Architecture (EA) Workgroup. On May 2001, Version 1 of the Enterprise Architecture Security Architecture Domain was produced. It was the COTS Privacy, Security and Access Workgroup who made 2001 Security Architectural to create anThe Department of Techn ... [1]

Deleted: MISSION AND OBJECTIVES

DRAFT

ENTERPRISE ARCHITECTURE CHANGE SUMMARY:

Ernie Steidle discussed the history behind the development of the Commonwealth's security standard, COV ITRM Standard SEC2001-01-1. He noted that on May 1, 2001 the COTS Enterprise Architecture (EA) Workgroup produced the Enterprise Architecture Security Domain, Version 1. The Department of Technology Planning, guided by the EA Security Domain, developed the information technology security standard, and companion security policy and guidelines. These documents were promulgated on December 7, 2001 by the Secretary of Technology.

Steidle reminded the members that in the December meeting they were tasked to review the Commonwealth security standards and guidelines from the perspective of their agencies and recommend changes (e.g., guidelines that should become standards, standards that should become guidelines, as well as new/additional standards or guidelines). As a result of the planned consolidated IT environment under the Virginia Information Technology Agency (VITA), Workgroup members discussed the benefits and limitations of relieving agency heads of direct responsibility for IT security and placing such responsibility with the director of VITA.

SECURITY PROCESS BY STANDARD:

Ernie Steidle guided the discussion which covered placing all items (e.g., processes, standards, and guidelines) into an MS Access database readable by members on the SharePoint Web site, and limiting process development to only standards (currently there are 42 standards with more than one process suggested). Fourteen processes asked for University assistance and were aligned with training and certification. The Workgroup members affiliated with universities were asked to explore what services their institutions would be willing to provide and under what arrangements (e.g., free or for a fee)

Further discussion noted that the DTP Due Diligence database ties standards to IT assets and that an outcome of this work effort will be to tie processes to IT assets in order to tracked and manage them. Chuck Tyger will send Ernie Steidle related information from the Due Diligence database to begin the development process.

In order to complete the review and make recommendation to COTS at their March meeting, the Workgroup members agreed to hold three all day work sessions to finalize the security standards, security processes, and the security database tracking and management program (i.e., Standards – January 27 at 10:00 AM, Processes – February 3 at 10:00 AM, and Database – February 10 at 10:00 AM).

GAP ANALYSIS:

Ernie Steidle noted that the approach taken in the Gap Analysis was an attempt to determine the gaps in the state agencies' security standards and processes that might be filled with the various programs offered by institutions of higher education. The initial recommendation concerned training and incident alerts. Members associated with the Alliance were asked to review with their institutions what tools were available and how best to integrate them into this work effort.

OTHER ISSUES:

None.

ADJOURNMENT

The meeting adjourned at 5:30 p.m.

NEXT MEETING DATE:

February 20, 2003 2:00 – 5:00 p.m. at the DRS in the first floor Conference Room

PREPARED & SUBMITTED BY: Eric Perkins, DTP

Deleted: THE MISSION OF THE COTS SECURITY WORKGROUP IS TOHAS:¶
¶
<#>DEFINE THE SECURITY ENTITIES IN A STATEWIDE IT SECURITY PROGRAM¶
<#>ASSIST….PROTECT IT ASSETS¶
<#>COMMUNICATE IT SECURITY ALERTS AND BEST PRACTICES¶
<#>PROMOTE COORDINATION, COOPERATION AND INFORMATION SHARING AMONG IT AGENCIES¶
<#>DEFINE THE ENTITIES INVOLVED IN THE TECHNOLOGY SECURITY ISSUES¶
<#>CREATE ASSIST…. A STATEWIDE INFORMATION SECURITY OFFICE; AND¶
<#>DEVELOP EVALUATION TOOLS WHICH MEASURE COST SAVINGS ¶
¶
SHORT TERM OBJECTIVES

Deleted: :

Deleted: The Workgroup's primary role is to advise and assist entities in the executive branch of government that has the responsibility of IS activity. The Workgroup would act as an Advisory Council to these entities, exchanging information, advice and recommendations. ¶
¶
The COTS Security Workgroup's short term objectives are to assist in the define definition of the roles of Virginia Information Technology Technologies Agencies' Agency's (VITA) contributions to statewide Information Security, JMU, GMU and state agencies security. ¶
¶
Long Term Objectives:¶ … [2]

Deleted: ¶
APPROACHES

Deleted: Of the 13 components of the Standards and Best Practices identified, each has a process or certification to go through. The certification propert … [3]

Formatted: Bullets and Numbering

Deleted: ng.

Deleted: ¶

Deleted: NEXT MEETING DATE¶
¶
. January 16, 2003 3:00 – 5:00 p.m.¶
¶

Deleted: M

Deleted: 4:45

Deleted: .

Deleted: 3

Deleted: ¶

Deleted: Linda Taylor¶
DRS Information Services¶
(804) 662-7599¶
taylorlm@drs.state.va.us .

Page 1: [1] Deleted **PCSupport** **1/23/2003 10:23:00 AM**

COTS have has existed for a long time—there are eight or nine workgroups. One of the workgroups that produced products relative to technology security is the COTS Enterprise Architecture (EA) Workgroup. On May 2001, Version 1 of the Enterprise Architecture Security Architecture Domain was produced. It was the COTS Privacy, Security and Access Workgroup who made 2001 Security Architectural to create anThe Department of Technology Planning, guided by the EA Security Domain, developed the Information Technology Security Standard, December 7, 2001.

In each of the above documents, 13 security components were shared with different aspects of technology security. Associated with each 13 components were a series of Standards and Best Practices. In September 2002, the Commonwealth of Virginia (COV) Strategic Plan for Technology was introduced—an Initiative 2, Agency Project 2, to define a statewide security mission, entities and tasksprogram. The COTS Wworkgroup Structure structure was redefined— to align with the implementation of the Strategic Plan for Technology. As result, the Privacy, Security and Access Workgroup became the security Security workgroup Workgroupbecame an old privacy security …..

Page 2: [2] Deleted **PCSupport** **1/23/2003 11:00:00 AM**

The Workgroup's primary role is to advise and assist entities in the executive branch of government that has the responsibility of IS activity. The Workgroup would act as an Advisory Council to these entities, exchanging information, advice and recommendations.

The COTS Security Workgroup's short term objectives are to assist in the define definition of the roles of Virginia Information Technology Technologies Agencies' Agency's (VITA) contributions to statewide Information Security, JMU, GMU and state agencies security.

Long Term Objectives:

Once the statewide Information Technology Security Office is established,program takes place, the task is to enhance itassist in the implementation of the other parts of the Statewide Information Security Program. The role is to identify marketing and incentives for the Statewide Information Security Program for state agencies and for staff, identify the coordinating roles among Virginia Office of Preparedness and state colleges and universities, and identify the cost effectiveness of the security program.

Page 2: [3] Deleted **PCSupport** **1/23/2003 3:07:00 PM**

Of the 13 components of the Standards and Best Practices identified, each has a process or certification to go through. The certification properties of what (due diligent survey—computer network equipment, business applications and IT functions); who (technical owners, DPT staff person, functional program owner or agency head), why (ensure consistency) and how (procedures).

The Workgroup's task is to make up processes and decide which make sense, the least intrusive to its accomplishment of security and flexibility, and define and vote on the alternative processes to determine the best interest of its statewide technology program.

PROCESS DISCUSSION THIS SECTION NEEDS HELP— LOW VOLUME TAPE RECORDING BEGAN

13 Components → Standards → Best Practices

Standards and Best Practices will be merged. Other Standards and Best Practices can be added.
To develop new Standards and Best Practices, processes must be defined. List processes that currently match Standards and Best Practices used today.
In January, the workgroup will meet to finalize the recommendations for Standards and Best Practices.
Two possibilities: 1) tackle the Standards and Best Practices of the process—what exists, what you want to see, etc. and 2) suggest what the Standards and Best Practices are.
The priority order is not known at this time.
Identify whose responsibility to research critical incidents.

Starting point: use the ITM security Standards and Best Practices which already exist, been approved and been through the referee process. In order to add a Standard or Best Practice or recommend changes to the status from a Standard or Best Practice, you must reference another national or international Standards or Best Practices document (limit the way you identify an additional Standard and Best Practice), or to change a status of a Best Practice to a Standard or a Standard to a Best Practice.
Steps
Use the security component from the security architecture by taking the existing Standards of Best Practices of the security architecture and arrange them.
Recommend a standard becomes a Best Practice or a Best Practice becomes a standard.
Add a standard or Best Practice if there is reference to a national or international standard document to justify
Use the Standards and Practices to identify the processes already exists or processes that would help manifest Standards and Best Practices; but not go into what, who, how and why.

TIME LINE

December, 2002

January 9, 2003
Last date to provide component Standards and Business Practices data. Ernie will post on shared site within 12 business days.and provide issues analysis for discussion at the 01/16/03 meeti